

Когнитивное отображения сети POS-устройств для эффективного мониторинга происходящих в ней событий и процессов

Д.В. Козлов¹, Н.П. Садовникова¹, Л.В. Дружинина¹, Д.В. Петрова²

¹ Волгоградский государственный технический университет,

² Московский технологический университет

mrdiko4@gmail.com, sadovnikova@vstu.ru, deli_86@mail.ru,
darina200896@mail.ru

Аннотация

В статье описываются основные проблемы при мониторинге работы POS-сетей. Рассматривается актуальность задачи разработки нового способа когнитивного отображения сети POS-устройств для эффективного мониторинга происходящих в них процессов. Формулируются основные требования к данной задаче. Предлагаются и описываются методы и алгоритмы, способные устранить актуальные проблемы при решении задачи мониторинга большого количества POS-устройств.

Ключевые слова: мониторинг, информационная система, POS-сети, когнитивное представление, графовые модели, поток событий

1. Введение

Сегодня система электронных платежей является сложной структурой, с множеством разнородных подсистем и элементов, распределенной на большой территории и требующей серьезных ресурсов для поддержания своего функционального состояния. Техническое и программное сопровождение данной системы сталкивается с рядом проблем, среди которых одновременная обработка данных большого объема, проблема безопасности осуществления электронных платежей, а также необходимость контроля корректности функционирования большого количества программных и аппаратных подсистем, взаимодействующих между собой. Мошенничество в сфере электронных платежей становятся все более актуальной проблемой в связи с ростом безналичных расчетов, появлением новых угроз и способов несанкционированного доступа к информации в POS-сетях. Защита информации в процессе осуществления платежных операций требует более строго контроля и обнаружения угроз в оперативном режиме. От скорости обнаружения и реагирования на киберугрозы зависит то, сможет ли система предотвратить утечку критически важной информации или нет. Проблему усугубляет постоянно возрастающая топологическая сложность сетей, которые образуют программные и аппаратные подсистемы POS.

На сегодняшний день существует большое количество методов автоматизированного обнаружение киберугроз [1]. Эти методы делятся на два основных класса: статистические методы [2] и методы искусственного интеллекта [3]. При этом наиболее эффективно обнаруживать угрозы и предотвращать утечку информации, способны только комплексные решения, сочетающие методы автоматического обнаружения угроз и методы, реализующие проактивное управление системой безопасности POS-сети [4].

Одним из решений, позволяющих значительно снизить риски, может стать внедрение единой информационной системы администрирования POS-сетей и ее интеграция с сервисом проактивного мониторинга [5]. Сервис мониторинга позволяет оперативно обнаружить угрозы безопасности и эффективно их устранить. Реализация сервиса мониторинга, позволяющего осуществлять сбор и предоставление оператору POS-сети информацию о существующих угрозах и параметрах сети в реальном времени, способна максимально сократить время обнаружения атак и даже предотвратить их появление [6] [7]. С помощью современных технологий, таких как: базы данных реального времени и realtime web, возможно обнаружение киберугроз и своевременное информирование о них лиц, принимающих решения (операторов системы администрирования POS-сетей) [8].

При реализации сервиса мониторинга, оператор в реальном времени получит доступ ко всем событиям и процессам, происходящим в POS-сети. Однако, это повысит эффективность обнаружения угроз, только в том случае, если оператор будет иметь возможность соотнести каждое событие, с конкретным устройством и процессом его породившем. Сложность задачи классификации событий связана с несколькими факторами:

- большое количество событий. Человеку просто невозможно анализировать такой объем информации в реальном времени;
- большое количество различных типов процессов, происходящих в системе. Сопоставление события с конкретным процессом определенного типа, зачастую требует детального анализа параметров данного события и представляет сложность для оператора;
- сложная топология современных POS-сетей. Зачастую, событие принадлежит процессу, происходящему не в одном устройстве, а сразу в нескольких связанных между собой устройствах, или даже в группе устройств, содержащей как связанные, так и не связанные устройства. В данном случае соотнесение конкретного события, произошедшего на конкретном устройстве, с процессом охватывающим группу устройств, с учетом топологии сети образованной данной группой устройств, является нетривиальной задачей.

Следовательно, организация эффективного мониторинга возможна, только при наличии инструмента, позволяющего осуществлять фильтрацию потока событий, сопоставлять события с конкретным процессом и со всеми связанными с ним структурными элементами POS-сети (с учетом их топологии). Для реализации такого инструмента предлагается использовать метод когнитивного представления топологии POS-сети и событий, связанных с ее элементами. Такой подход позволит решить поставленные задачи и существенно сократить время на выявление угроз, их анализ и предотвращение.

2. Топология POS-сети и ее структурные элементы

POS-сеть представляет собой множество программных и аппаратных решений, осуществляющих платежные операции, либо участвующие в их обеспечении. К аппаратным решениям относятся платежные терминалы, пинпады, ридеры и другие устройства различных моделей. При этом существуют модели устройств, способные выполнять несколько из перечисленных функций или все одновременно. Существуют и программные решения, выполняемые на персональных компьютерах и берущие на себя часть функций терминала. Каждое из аппаратных решений в дальнейшем будем именовать физическим устройством (ФУ).

Зачастую, имеется возможность физического соединения нескольких ФУ между собой. Примером, таких соединений могут быть соединение терминала и пинпада или пинпада и ридера. Одной физической связью соединяется между собой пара устройств: управляющее и управляемое. Несколько связанных устройств образуют комплекс устройств. Структура комплекса устройств, как правило иерархична и древовидна: комплекс устройств имеет одно главное устройство — корень комплекса, каждое управляемое устройство имеет всего одно управляющее.

Каждое из физических устройств, в свою очередь, имеет собственное программное обеспечение. Например, для корректной работы терминала необходимо ПО, осуществляющее платежные операции в обслуживаемом его банке-эквайере. Такое программное обеспечение в дальнейшем будем называть логическим устройством (ЛУ). Важным является тот факт, что существуют устройства способные работать с несколькими банками-эквайерами одновременно (мультибанкинг) либо же работающих с несколькими валютами. В таком случае, работа с каждым из банков и с каждой из валют требует своего ПО, выполняемого на устройстве. Из этого следует, что одному физическому устройству соответствует одно или более логических устройств.

Исходя из вышеизложенного видно, что каждое из логических устройств связано с банком-эквайером. Данная связь осуществляется за счет наличия у владельца физического устройства, счета в банке (Account). Владельца банковского счета в дальнейшем будем именовать Customer — клиент, владелец счета/счетов в банке-эквайере.

Merchant — юридическое лицо, которое осуществляет свою деятельность в сфере продажи товаров и предоставления услуг. Merchant может принимать к оплате платежные карты с использованием платежных терминалов. Каждое логическое устройство привязано к соответствующему ему Merchant'у.

Customer может иметь один или более Merchant'ов.

Кроме того, Customer и Merchant имеют физические адреса, причем адрес Customer'a — юридический адрес владельца счетов, а адрес Merchant'a — адрес по которому расположены физические устройства Merchant'a.

3. Формулировка требований

Для организации эффективного мониторинга сети POS-устройств, необходимо чтобы оператор имел возможность получать как максимально общую информацию о ее работе, так и детальную информацию о работе каждого из процессов, происходящих в ней.

Для получения обобщенной информации о работе сети, необходимо отображать оператору структуру сети, критические моменты и обобщенные интегральные характеристики ее работы, требующие внимания оператора.

В свою очередь, для получения детальной информации о работе того или иного процесса в сети POS-устройств, необходимо создать гибкую систему фильтров получаемой оператором информации. Основная часть получаемой оператором информации — это события, происходящие в POS-сети. Следовательно, необходимо решить задачу фильтрации общего потока событий, а также классификации событий на типовые процессы и подпроцессы.

4. Выбор способа отображения

Для выполнения поставленных требований, в первую очередь, необходимо выбрать способ отображения структуры POS-сети и процессов, происходящих в ней.

Как видно из описания структуры и топологии POS-сети физические и логические устройства имеют следующие связи: ФУ — ФУ (один ко многим) и ФУ — ЛУ (один ко многим). Данное множество связей можно полностью отобразить в виде дерева, где вершины дерева — физические или логические устройства, а дуги — физические или логические соединения. Однако, для полноты картины, оператору также необходимо предоставлять информацию о сопутствующих понятиях, важных с точки зрения процессов, происходящих в POS-сети. К таким понятиям относятся, уже описанные ранее: Merchant, Account, Customer, а также физические адреса устройств и юридические адреса Customer'ов. Кроме того, для большей наглядности из адреса можно дополнительно выделить три сущности: Город, Регион и Страна. В сущности Адрес оставим, только поля улицу, номер дома и почтовый индекс. При этом к предыдущим видам связей, добавляются новые. Выпишем их:

- ФУ (один) — (много) ФУ;
- ФУ (один) — (много) ЛУ;
- Merchant (один) — (много) ЛУ;
- Account (один) — (много) Merchant;
- Customer (один) — (много) Account;
- Адрес (один) — (много) Customer;
- Адрес (один) — (много) Merchant;
- Адрес (один) — (много) ФУ;
- Город (один) — (много) Адрес;
- Регион (один) — (много) Город;
- Страна (один) — (много) Регион.

Подобный перечень связей в своей совокупности образует граф. Следовательно, для полноты отображения всех сущностей и связей между ними необходимо использовать графовую модель.

5. Описание метода отображения

Для отображения каждой из вершины графа, в первую очередь, необходимо выбрать ее идентификатор, для его отображения оператору в виде текста. Этот идентификатор должен быть уникальным и позволять оператору отличать один объект от другого объекта подобного класса. Опишем эти идентификаторы для каждого класса объектов:

- Физическое устройство — серийный номер устройства;
- Логическое устройство — уникальный строковый идентификатор Terminal Id;
- Merchant - уникальный строковый идентификатор Merchant Id;
- Account - уникальный строковый идентификатор Account Id;
- Customer - уникальный строковый идентификатор Customer Id;
- Адрес — строка, содержащая название улицы и номер дома;
- Город — название города;
- Регион — название региона;
- Город (один) — (много) Адрес;
- Регион (один) — (много) Город;
- Страна — название страны.

Для того, чтобы оператор мог отличить различные классы объектов друг от друга, будем обозначать их графически, т.е. присвоим каждому из классов свою пиктограмму. При этом необходимо, выбрать максимально простые графические объекты, для того чтобы они не отвлекали оператора. Стоит также заметить, что описано девять (9) классов объектов. 9 — пограничное число в так называемом «кошельке Миллера» и большинству людей будет очень сложно удержать такое количество объектов во внимании одновременно.

Как показал в 1956 г. Дж. А. Миллер, человек способен удерживать в кратковременной памяти не более 7 ± 2 предметов. Этот принцип и получил название «кошелёк Миллера» [9] [10]. 7 ± 2 — число факторов которыми одновременно может оперировать человек в своей текущей деятельности. Однако наиболее комфортно человеку работать с еще меньшим количеством объектов. При одновременной работе с 4–5 факторами человек способен достаточно продолжительное время выполнять возложенные на него функции совершая минимальное количество ошибок.

В настоящее время принцип «кошелька Миллера» широко используется при построении графических интерфейсов пользователя [11]. Одной из ключевых особенностей использования этого принципа является его иерархичность: каждый из 7 ± 2 объектов, используемых человеком в процессе его работы, может быть разбит на 7 ± 2 дочерних объекта без существенного ущерба для производительности. При такой иерархической структуре объектов, человеку достаточно легко оперировать 7 ± 2 объектами именно того уровня, который ему необходим в текущий момент времени, и переключаться

на другой уровень в случае необходимости. Важно отметить, что количество таких уровней также ограничено «кошельком Миллера» и не должно превышать 7 ± 2 .

Таким образом, для сокращения количества пиктограмм, служащих для отображения класса объектов, выделим из них 4 группы классов:

- Физические устройства;
- Логические устройства;
- Владельцы устройств (Merchant, Account, Customer);
- Географическое расположение устройств (Адрес, Город, Регион, Страна).

Для того чтобы разделить для оператора описанные группы объектов необходимо выделить их общим графическим признаком. Таким признаком может быть цвет. При этом, стоит отметить, что цвета для отображения графа по умолчанию лучше выбирать в сине-зеленом спектре. Эти цвета являются более «спокойными» и человек меньше устает от них. Желтые и красные части спектра будут использоваться для отображения предупреждений и ошибок. В то же время цвета должны быть сочетающимися между собой, поэтому лучше всего воспользоваться специальной палитрой цветов «Between blue and green» [12]. В данную палитру входят следующие цвета: `rgb(#00bde7)`, `rgb(#00d8d4)`, `rgb(#008ba0)`, `rgb(#00d6b2)`, `rgb(#00afa3)`. В таблице 1 представлены группы объектов и соответствующие им цвета.

Таблица 1. Цвета групп объектов

Группа объектов	Цвет
Физические устройства	#00bde7
Логические устройства	#00d8d4
Владельцы устройств	#008ba0
Географическое расположение устройств	#00afa3

В свою очередь, для отображения классов объектов были выделены 7 пиктограмм, приведенные на рисунке 1.






Рис. 1. Пиктограммы для отображения классов объектов

Каждая из пиктограмм, представленных на рисунке 1, может иметь закрашенную версию (с заливкой внутри контура), что дает в два раз больше типов пиктограмм. Это используется, например, для отображения управляющих устройств внутри комплекса устройств. Стоит отметить, что если комплекс состоит из одного ФУ, то это единственное устройство также является управляющим и отображается закрашенной пиктограммой.

В таблице 2 представлены классы объектов и соответствующие им пиктограммы.

Как видно из таблицы 2, вершина класса объекта «Регион» имеет цвет `rgb(#00d6b2)` и он отличен от группы «Географическое расположение устройств». Это сделано для того чтобы визуально отделить класс «Регион» от класса «Страна» и при этом использовать ту же пиктограмму.

Таблица 2. Графическое отображение классов объектов

Класс	Цвет	Закрашена	Пиктограмма
Управляющее физическое устройство	#00bde7	да	
Управляемое физическое устройство	#00bde7	нет	
Логическое устройств	#00d8d4	нет	
Merchant	#008ba0	нет	
Account	#008ba0	нет	
Customer	#008ba0	нет	
Адрес	#00afa3	нет	
Город	#00afa3	нет	
Регион	#00d6b2	да	
Страна	#00afa3	да	

Кроме особого отображения для вершин каждого из классов объектов дополнительно стилизуются и связи между ними. Некоторые связи, например, связи типа ФУ — ФУ необходимо сделать более заметными для оператора, т.к. он в первую очередь следит именно за физическими и логическими устройствами. Следовательно, связи необходимо проранжировать по степени «заметности» для внимания оператора. Цвет связи соответствует цвету вершины, к которой связь проведена. В таблице 3 представлены связи между классами объектов и их графическое отображение.

Описав способ отображения связей и объектов, можно привести пример отображения POS-сети для оператора системы мониторинга. Пример представлен на рисунке 2.

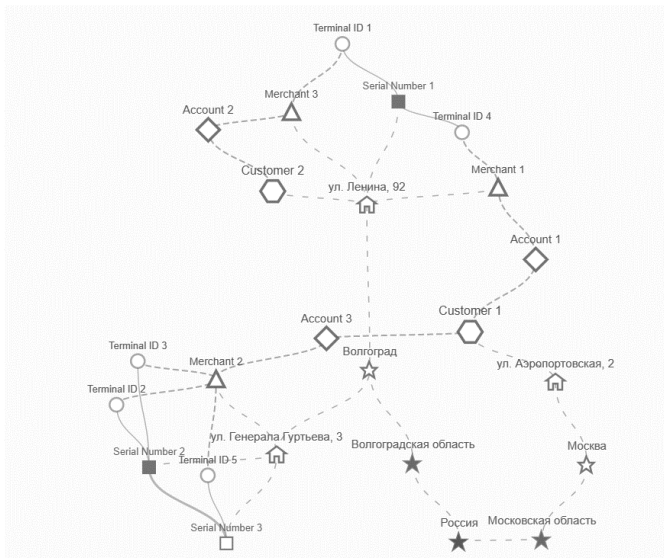


Рис. 2. Пример отображения POS-сети

Для более детального отображения того или иного процесса в POS-сети необходимо предоставить оператору сервиса мониторинга набор инструментов фильтрации отображаемой области POS-сети и событий, происходящих в ней. К таким инструментам относятся:

- фильтр отображаемых классов объектов;
- фильтр объектов по ключевому полю каждого из классов объектов;
- фильтр событий по типу событий (информация, предупреждение, ошибка и др.);
- фильтр событий по классу процесса, к которому относится событие.

При фильтрации объектов в сервисе мониторинга POS-сети выбираются объекты, которые удовлетворяют всем введенным фильтрам, и оператору отображаются все выбранные и соединенные с ними объекты. Соединенные объекты выбираются из следующих иерархий как снизу-вверх, так и сверху-вниз:

- ФУ — ЛУ — Merchant — Account — Customer;
- ФУ — Адрес — Город — Регион — Страна;
- Merchant — Адрес — Город — Регион — Страна;
- Customer — Адрес — Город — Регион — Страна;
- управляющее ФУ — управляемое ФУ (при наличии фильтра «Фильтр по связанным ФУ»).

Таблица 3. Связи между классами объектов

Тип связи	Ранг связи	Способ отображения	Цвет	Графическое изображение
ФУ — ФУ	1	Сплошная линия двойной толщины	#00bde7	
ФУ — ЛУ	2	Сплошная линия одинарной толщины	#00d8d4	
ЛУ — Merchant Merchant — Account Account — Customer	3	Пунктирная линия одинарной толщины. Расстояние между штрихами одинарное	#008ba0	
ФУ — Адрес Merchant — Адрес Customer — Адрес Адрес — Город Город — Регион Регион — Страна	4	Пунктирная линия одинарной толщины. Расстояние между штрихами двойное	#00afa3	

При фильтрации по классу объектов, объекты, которые не выбраны в фильтре не отображаются, а устройства, находящиеся ниже по иерархии, связываются с устройствами, находящимися выше по иерархии.

Интерфейс фильтров, а также пример фильтрации представлен на рисунке 3.

Кроме того, для уменьшения количества отображаемых объектов в сервисе мониторинга при большом количестве устройств предусмотрен алгоритм сворачивания вершин графа отображения POS-сети. При сворачивании вершины графа, все вершины, находящиеся ниже по иерархии, не отображаются. На рисунке 4 приведен пример свертки вершины класса объекта Customer.

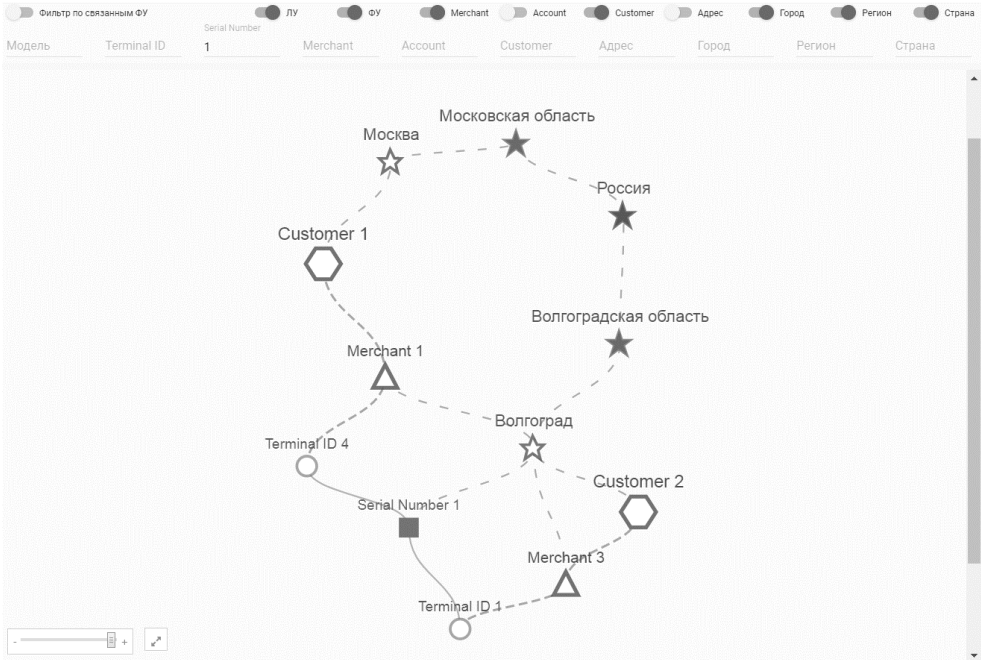


Рис. 3. Пример использования фильтров в сервисе мониторинга

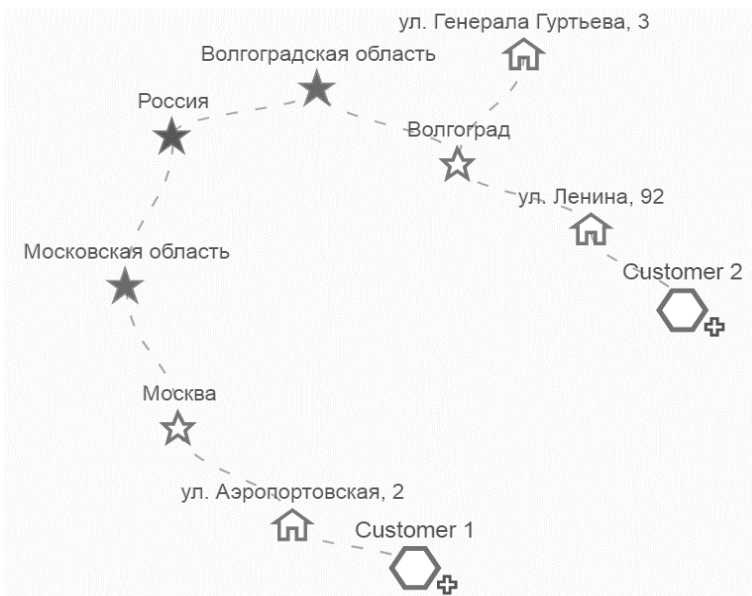


Рис. 4. Пример свертки узлов графа отображения POS-сети

6. Заключение

В результате работы был проведен анализ задач администрирования POS-сетей, выявлены особенности процессов управления их безопасностью. Формализованы основные структурные элементы POS-сети, их ключевые характеристики и отношения между ними. Предложен метод когнитивного отображения сети POS-устройств, а также алгоритмы фильтрации и свертки вершин графа. Совокупность предложенных методов и алгоритмов, позволяет оператору сервиса мониторинга своевременно получать необходимую информацию, за счет наглядного представления элементов POS сети и всех имеющихся связей между ее объектами. В то же время гибкая система фильтрации отображаемых объектов POS-сети, позволяет оператору сфокусироваться только на тех объектах, информация о которых необходима для решения текущей задачи.

Интеграция системы мониторинга с реализованным методом когнитивного отображения POS-сети в процессе администрирования работы POS-устройств, позволит сократить время на обнаружение угроз безопасности для конкретных устройств и всей сети в целом. Это в свою очередь, позволит сократить количество успешных мошеннических атак в системе и уменьшит издержки по их нивелированию. Кроме того, предложенный метод позволит сократить объем трудозатрат на анализ текущего состояния системы за счет автоматизации процесса сбора детальной информации о каждом происходящем событии.

Литература

- [1] Palshikar G.K. The Hidden Truth — Frauds and Their Control: A Critical Application for Business Intelligence // *Intelligent Enterprise*. 2002. Vol.5, No. 9. P. 46–51.
- [2] Bolton R., Hand D. Statistical Fraud Detection: A Review (With Discussion) // *Statistical Science*. 2002. Vol. 17(3). P. 235–255.
- [3] Estevez P., Held C., Perez C. Subscription fraud prevention in telecommunications using fuzzy rules and neural networks // *Expert Systems with Applications*. 2006. Vol. 31. P. 337–344.
- [4] ACFE. Report to the Nations on Occupational Fraud and Abuse, 2018.
- [5] Козлов Д. В. Концепция системы контроля безопасности функционирования POS-сетей в реальном времени / Д.В. Козлов, Н.П. Садовникова // *Информационное общество: образование, наука, культура и технологии будущего*. Выпуск 1 (Труды XX Международной объединенной научной конференции «Интернет и современное общество», IMS-2017, Санкт-Петербург, 21 – 23 июня 2017 г. Сборник научных статей). СПб: Университет ИТМО, 2017. С. 44-51.
- [6] Предотвращение мошенничества в системах электронных платежей на основе мониторинга и анализа событий в POS-сетях = Fraud prevention in the system of electronic payments on the basis of monitoring and analysis events in POS-networks [Электронный ресурс] / Д.В. Козлов, Н.П. Садовникова, Л.В. Дружинина, Д.В. Петрова // *International Journal of Open Information Technologies*. 2017. Vol. 5. № 11. С. 15-20. URL: <http://injoit.org/index.php/j1/article/view/503/475>.
- [7] Fraud prevention in the system of electronic payments on the basis of POS-networks security monitoring / О.А. Авдеюк, Д.В. Козлов, Л.В. Дружинина, И.А. Тарасова // *IEEE Tenth International Conference «Management of large-scale system development» (MLSD'2017) (Moscow, Russia, October 2-4, 2017): Proceedings* / V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, IEEE (Institute of Electrical and Electronics Engineers). 2017. 4 p. DOI: 10.1109/MLSD.2017.8109597.
- [8] Анализ существующих технологий для реализации облачного мониторинга POS-сетей / О.А. Авдеюк, Л.В. Дружинина, Д.В. Козлов, И.А. Тарасова // *Управление развитием крупномасштабных систем (MLSD'2017): матер. десятой междунар. конф. (г. Москва, 2-4 октября 2017 г.)*. В 2 т. Т. II. Секции 5–13 / под общ. ред. С.Н. Васильева, А.Д.

- Цвиркуна; ФГБУН «Ин-т проблем управления им. В.А. Трапезникова» РАН. Москва, 2017. С. 312-314.
- [9] Миллер Дж. А. Магическое число семь плюс или минус два: О некоторых пределах нашей способности перерабатывать информацию // Инженерная психология: Сб. статей. М.: Прогресс, 1964. С. 192-225.
- [10] Солсо Р. Л. Когнитивная психология. М.: Тривола, 1996. С. 149-196.
- [11] Ефремов А. С. Применение способов прототипирования пользовательских интерфейсов при создании электронных образовательных ресурсов средствами веб-технологий в обучении будущих учителей // Мир науки, культуры, образования. Горно-Алтайск: МНКО, 2017. № 2(63). С. 88-91.
- [12] Цветовая палитра «Between blue and green». URL: <http://www.color-hex.com/color-palette/4465> (дата обращения: 23.02.2018).

Cognitive Mapping of POS-Devices Network for Effective Monitoring of Events and Processes Occurring in it

D.V. Kozlov¹, N.P. Sadovnikova¹, L.V. Druzhinina¹, D.V. Petrova²

¹ Volgograd State Technical University, ² Moscow Technical University

The article describes the main problems when monitoring the operation of POS networks. The urgency of the developing task a new method of POS-devices network cognitive mapping for effective monitoring of processes occurring in them is considered. The main requirements to this problem are formulated. Methods and algorithms that can eliminate actual problems when solving the task of monitoring a large number of POS-devices are proposed and described.

Keywords: monitoring, information system, POS networks, cognitive representation, graph models, event flow